Some Recent Progress in Lattice-Based Cryptography

Chris Peikert

SRI International

Abstract. The past decade in computer science has witnessed tremendous progress in the understanding of *lattices*, which are a rich source of seemingly hard computational problems. One of their most promising applications is to the design of cryptographic schemes that enjoy exceptionally strong security guarantees and other desirable properties.

Most notably, these schemes can be proved secure assuming only the *worst-case* hardness of well-studied lattice problems. Additionally, and in contrast with number-theoretic problems typically used in cryptography, the underlying problems have so far resisted attacks by *subexponential-time* and *quantum* algorithms. Yet even with these security advantages, lattice-based schemes also tend to be remarkably simple, asymptotically efficient, and embarrassingly parallelizable.

This tutorial will survey the foundational results of the area, as well as some more recent developments. Our particular focus will be on the core hard cryptographic (average-case) problems, some recurring techniques and abstractions, and a few notable applications.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-642-00457-5_36

O. Reingold (Ed.): TCC 2009, LNCS 5444, p. 72, 2009.